

日本国特許庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年 7月 4日

出願番号

Application Number:

特願2001-202954

出願人

Applicant(s):

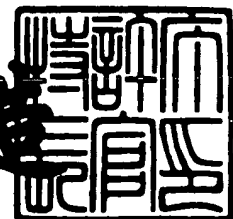
アライドテレシス株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月31日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3078299

【書類名】 特許願

【整理番号】 IP217001

【提出日】 平成13年 7月 4日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/32
H04L 12/28
G06F 13/00

【発明者】

【住所又は居所】 東京都品川区西五反田 7 - 2 1 - 1 1 アライドテレシ
ス株式会社内

【氏名】 佐藤 貴之

【特許出願人】

【識別番号】 396008347

【氏名又は名称】 アライドテレシス株式会社

【代理人】

【識別番号】 100099818

【弁理士】

【氏名又は名称】 安孫子 勉

【手数料の表示】

【予納台帳番号】 064699

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 インテリジェント中継機器における不正アクセス回避方法、
インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中
継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中
継機器及びLANシステム

【特許請求の範囲】

【請求項1】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器における不正アクセス回避方法であって、

外部の機器からのアクセスが前記TCP/IPプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元IPアドレスを抽出して記憶し、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元IPアドレスが前記記憶された送信元IPアドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元IPアドレスを有する外部の機器と前記インテリジェント中継機器間の以後の通信を可能とすることを特徴とするインテリジェント中継機器における不正アクセス回避方法。

【請求項2】 送信元IPアドレスが一致しないと判定された場合、その一致しないと判定された送信元IPアドレスを不正アクセスIPリストに登録することを特徴とする請求項1記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項3】 送信元IPアドレスが一致しないと判定された場合、その一致しないと判定された送信元IPアドレスを、認証を受けた管理用コンピュータへ通知することを特徴とする請求項1又は請求項2記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項4】 送信元IPアドレスが一致すると判定された場合、当該送信元IPアドレスが予め設定された有効期限内のものであるか否かを判定し、有効期限内のものであると判定された場合にのみ当該送信元IPアドレスを有する外

部の機器とインテリジェント中継機器間の以後の通信を可能とすることを特徴とする請求項 1 記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項 5】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から TCP / IP プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる TCP / IP プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 IP アドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 IP アドレスが、前記記憶された送信元 IP アドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第 7 のステップと、

前記外部の機器の送信元 IP アドレスと前記記憶された送信元 IP アドレスと

が一致するか否かの判定において、一致すると判定された場合には、送信元 I P アドレスが記憶されている送信元 I P アドレスと一致すると判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 8 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 9 のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項 6】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 I P アドレスを前記インテリ

ジェント中継機器に抽出せしめると共に、記憶せしめる第5のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第6のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元IPアドレスが、前記記憶された送信元IPアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第7のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元IPアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第8のステップと、

前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元IPアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第2のステップから前記インテリジェント中継機器へ実行せしめる第9のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元IPアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第10のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項7】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第1のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるTCP/IPプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第2のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第3のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第4のステップと、

前記第4のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元IPアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第5のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第6のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元IPアドレスが、前記記憶された送信元IPアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第7のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元IPアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第8のステップと、

前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元IPアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とす

ると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 9 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、前記インテリジェント中継機器に記憶せしめる第 1 0 のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項 8】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記

外部の機器からのパケット中に含まれている送信元 I P アドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 I P アドレスが、前記記憶された送信元 I P アドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第 7 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元 I P アドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第 8 のステップと、

前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元 I P アドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 9 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知せしめる第 1 0 のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項 9】 第 1 0 のステップで応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知せしめる第 1 1 のステップを具

備してなることを特徴とする請求項 7 記載のインテリジェント中継機器用不正アクセス回避プログラム。

【請求項 1 0】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から TCP / IP プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる TCP / IP プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 IP アドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 IP アドレスが、前記記憶された送信元 IP アドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第 7 のステップと、

前記外部の機器の送信元 IP アドレスと前記記憶された送信元 IP アドレスと

が一致するか否かの判定において、一致すると判定された場合には、送信元 I P アドレスが記憶されている送信元 I P アドレスと一致すると判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 8 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 9 のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項 1 1】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 I P アドレスを前記インテリ

ジェント中継機器に抽出せしめると共に、記憶せしめる第5のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第6のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元IPアドレスが、前記記憶された送信元IPアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第7のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元IPアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第8のステップと、

前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元IPアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第2のステップから前記インテリジェント中継機器へ実行せしめる第9のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元IPアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第10のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項12】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第1のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるTCP/IPプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第2のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第3のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第4のステップと、

前記第4のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元IPアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第5のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第6のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元IPアドレスが、前記記憶された送信元IPアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第7のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元IPアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第8のステップと、

前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元IPアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とす

ると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 9 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、前記インテリジェント中継機器に記憶せしめる第 1 0 のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項 1 3】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第 1 のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記

外部の機器からのパケット中に含まれている送信元 I P アドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 I P アドレスが、前記記憶された送信元 I P アドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第 7 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元 I P アドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第 8 のステップと、

前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元 I P アドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第 2 のステップから前記インテリジェント中継機器へ実行せしめる第 9 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知せしめる第 1 0 のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項 1 4】 第 1 0 のステップで応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知せしめる第 1 1 のステップを

具備してなることを特徴とする請求項 1 2 記載のコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項 1 5】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部の機器からのアクセスが前記 T C P / I P プロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元 I P アドレスを抽出して前記記憶部に記憶せしめ、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元 I P アドレスが前記記憶された送信元 I P アドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元 I P アドレスを有する外部の機器との以後の通信が可能となるよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項 1 6】 中央制御部は、送信元 I P アドレスが一致しないと判定された場合、その一致しないと判定された送信元 I P アドレスを記憶部の不正アクセス I P リストに登録することを特徴とする請求項 1 5 記載のインテリジェント中継機器。

【請求項 1 7】 中央制御部は、送信元 I P アドレスが一致しないと判定された場合、その一致しないと判定された送信元 I P アドレスを、認証を受けた管理用コンピュータへ通知することを特徴とする請求項 1 5 又は請求項 1 6 記載のインテリジェント中継機器。

【請求項 1 8】 中央制御部は、送信元 I P アドレスが一致すると判定され

た場合、当該送信元 I P アドレスが予め設定された有効期限内のものであるか否かを判定し、有効期限内のものであると判定された場合にのみ当該送信元 I P アドレスを有する外部の機器とインテリジェント中継機器間の以後の通信を可能とすることを特徴とする請求項 1 5 記載のインテリジェント中継機器。

【請求項 1 9】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、 L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第 1 のステップと、

前記第 1 のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を行う第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 I P アドレスを抽出すると共に、当該送信元 I P アドレスを前記記憶部に記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、

前記外部の機器に対する以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 I P アドレスが、前記記憶された送信元 I P アドレスと一致するか否かを判定する第 7 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致すると判定された場合には、送信元 I P アドレスが記憶されている送信元 I P アドレスと一致すると判定された外部の機器に対する以後の応答を可能とすると共に、前記第 2 のステップからの実行へ移行する第 8 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元 I P アドレスが一致しないと判定された外部の機器に対する以後の応答を不可とする第 9 のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項 2 0】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第 1 のステップと、

前記第 1 のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づい

た認証処理を行う第2のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第3のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第4のステップと、

前記第4のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元IPアドレスを抽出すると共に、当該送信元IPアドレスを前記記憶部に記憶せしめる第5のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第6のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元IPアドレスが、前記記憶された送信元IPアドレスと一致するか否かを判定する第7のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元IPアドレスが所定の有効期限内のものであるか否かを判定する第8のステップと、

前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元IPアドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第2のステップからの実行へ移行する第9のステップと、

前記外部の機器の送信元IPアドレスと前記記憶された送信元IPアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元IPが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元IPアドレスが一致しないと判定された外部の機器に対する以後の応答を不可とする第10のス

テップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項 2 1】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第 1 のステップと、

前記第 1 のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる T C P / I P プロトコルに基づいた認証処理を行う第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 I P アドレスを抽出すると共に、当該送信元 I P アドレスを前記記憶部に記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではない

と判定された場合に、当該アクセスのあった外部の機器の送信元 I P アドレスが、前記記憶された送信元 I P アドレスと一致するか否かを判定する第 7 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元 I P アドレスが所定の有効期限内のものであるか否かを判定する第 8 のステップと

前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元 I P アドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第 2 のステップからの実行へ移行する第 9 のステップと、

前記外部の機器の送信元 I P アドレスと前記記憶された送信元 I P アドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、前記記憶部に記憶せしめる第 1 0 のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項 2 2】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第 1 のステップと、

前記第 1 のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによる TCP / IP プロトコルに基づいた認証処理を行う第 2 のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第 3 のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第 4 のステップと、

前記第 4 のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元 IP アドレスを抽出すると共に、当該送信元 IP アドレスを前記記憶部に記憶せしめる第 5 のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第 6 のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元 IP アドレスが、前記記憶された送信元 IP アドレスと一致するか否かを判定する第 7 のステップと、

前記外部の機器の送信元 IP アドレスと前記記憶された送信元 IP アドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元 IP アドレスが所定の有効期限内のものであるか否かを判定する第 8 のステップと、

前記送信元 IP が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元 IP アドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第 2 のステップからの実行へ移行する第 9 のステップと、

前記外部の機器の送信元 IP アドレスと前記記憶された送信元 IP アドレスと

が一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元 I P が所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元 I P アドレスが一致しないと判定された外部の機器に対する以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知する第 1 0 のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項 2 3】 第 1 0 のステップで応答不可とされた外部の機器の送信元 I P アドレスを、所定の管理用コンピュータへ通知する第 1 1 のステップを具備してなることを特徴とする請求項 2 1 記載のインテリジェント中継機器。

【請求項 2 4】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、 L A N 基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなる L A N システムであって、

前記インテリジェント中継機器は、請求項 1 5 記載のインテリジェント中継機器であることを特徴とする L A N システム。

【請求項 2 5】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、 L A N 基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなる L A N システムであって、

前記インテリジェント中継機器は、請求項 1 6 記載のインテリジェント中継機器であることを特徴とする L A N システム。

【請求項 2 6】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、 L A N 基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなる L A N システムであって、

前記インテリジェント中継機器は、請求項17記載のインテリジェント中継機器であることを特徴とするLANシステム。

【請求項27】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるLANシステムであって、

前記インテリジェント中継機器は、請求項18記載のインテリジェント中継機器であることを特徴とするLANシステム。

【請求項28】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるLANシステムであって、

前記インテリジェント中継機器は、請求項19記載のインテリジェント中継機器であることを特徴とするLANシステム。

【請求項29】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるLANシステムであって、

前記インテリジェント中継機器は、請求項20記載のインテリジェント中継機器であることを特徴とするLANシステム。

【請求項30】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるLANシステムであって、

前記インテリジェント中継機器は、請求項21記載のインテリジェント中継機

器であることを特徴とする LAN システム。

【請求項 3 1】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から TCP / IP プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN 基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなる LAN システムであって、

前記インテリジェント中継機器は、請求項 2 2 記載のインテリジェント中継機器であることを特徴とする LAN システム。

【請求項 3 2】 複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から TCP / IP プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、LAN 基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなる LAN システムであって、

前記インテリジェント中継機器は、請求項 2 3 記載のインテリジェント中継機器であることを特徴とする LAN システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、いわゆる LAN (Local Area Network) システムにおいて、パケットの中継機能などを有してなる中継機器に係り、特に、外部からの動作管理などが可能に構成されてなるいわゆるインテリジェント中継機器におけるセキュリティの向上等を図ったものに関する。

【0 0 0 2】

【従来の技術】

いわゆるハブやルータなどに代表されるいわゆるパケット中継機器は、LAN システムを構築する上で欠かせない機器であり、LAN システムの形態等に応じて、基本的な機能に加えて様々な機能を有するものが種々提案されている（例えば、特開平 5 - 3 2 7 7 2 0 号公報等参照）。このような中継機器において、特に、外部のコンピュータとの通信によって、その動作状況の把握や、動作条件の

設定などのいわゆる管理機能を有するものがあり、このような中継機器は、一般にインテリジェント中継機器と称されている。

従来、このようなインテリジェント中継機器を用いて構築された LAN システムにおいて、このインテリジェント中継機器の各種の動作条件等を、LAN システムに接続された管理用コンピュータからの遠隔操作により設定、変更する等の管理を可能とするために、インテリジェント中継機器には IP アドレスが付与されており、管理用コンピュータとインテリジェント中継機器間の通信処理には、いわゆる TCP / IP 通信処理が行われるようになっている。すなわち、具体的には、TELNET(RFC854)、SNMP(RFC1157)、TFTP(RFC1350)、ICMP(RFC792)、HTTP(RFC1945)などのいわゆる TCP / IP プロトコルが管理用コンピュータとインテリジェント中継機器間の通信の形態に応じて種々選択的に用いられるようになっている。

例えば、インテリジェント中継機器を、管理者以外の不正操作から防ぐために従来は、TELNET(RFC854)によって当該インテリジェント中継機器へログインできるようにし、ログイン後にユーザ識別子とパスワードを入力せしめ、それが所定のものと一致する場合にのみ管理者からのアクセスとして認証し、外部からのそれ以後の操作が許可されるようなものとなっていた。

【 0 0 0 3 】

【発明が解決しようとする課題】

しかしながら、このような従来の構成にあって、そのセキュリティはもっぱらプロトコルに依存するものであり、TCP / IP プロトコルの中には、セキュリティ機能を有しないものもあり、決して信頼性の高いセキュリティを保証するものではなかった。すなわち、上記従来装置の例で言えば、ログイン後のユーザ識別子とパスワードの入力による認証は、TELNETがその機能の一つとして有するものであり、インテリジェント中継機器への不正なアクセスを防止する観点から独自に付加された機能ではなく、しかも、ユーザ識別子とパスワードさえ一致していれば、管理用コンピュータ以外からのコンピュータからのアクセスであっても、容易に認証されてしまうという欠点があり、セキュリティの点で充分満足できるものではなかった。

【 0 0 0 4 】

本発明は、上記実状に鑑みてなされたもので、プロトコルのセキュリティ機能に依存することなく、しかも、予め指定されたコンピュータ以外からのアクセスを確実に断つことができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びLANシステムを提供するものである。

本発明の他の目的は、既存のソフトウェアに新たな機能を若干付加するだけで、セキュリティ機能の強化、ひいては信頼性の向上を図ることができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びLANシステムを提供することにある。

本発明の他の目的は、セキュリティに関するソフトウェアの簡素化を図ることができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びLANシステムを提供することにある。

【 0 0 0 5 】

【課題を解決するための手段】

上記発明の目的を達成するため、本発明に係るインテリジェント中継機器における不正アクセス回避方法は、

複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からTCP/IPプロトコルに基づいて管理可能に構成されるインテリジェント中継機器における不正アクセス回避方法であって、

外部の機器からのアクセスが前記TCP/IPプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元IPアドレスを抽出して記憶し、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元IPアドレスが前記記憶された送信元IPア

ドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元 I P アドレスを有する外部の機器と前記インテリジェント中継機器間の以後の通信を可能とするよう構成されてなるものである。

【 0 0 0 6 】

かかる方法においては、一旦、T C P / I P プロトコルによる認証が成立した後は、そのプロトコルの実行際に外部の機器から送信されたパケットに含まれている送信元 I P アドレスを抽出して記憶しておくことで、それ以後、外部の機器からアクセスが生じた際に、この送信元 I P アドレスが一致しない場合には、応答不可とされるため、ユーザ識別子とパスワードが一致していれば、送信元 I P アドレスが異なる場合であってもアクセスが可能になってしまうという従来の不都合が確実に回避でき、従来に比して、簡易な構成でより一層のセキュリティの向上が図られることとなるものである。

【 0 0 0 7 】

また、本発明の目的を達成するため、本発明に係るインテリジェント中継機器は、

複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器から T C P / I P プロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、L A N 基幹線とのインターフェイス機能を有する L A N 基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記 L A N 基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部の機器からのアクセスが前記 T C P / I P プロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元 I P アドレスを抽出して前記記憶部に記憶せしめ、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元 I P ア

ドレスが前記記憶された送信元 I P アドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元 I P アドレスを有する外部の機器との以後の通信が可能となるよう構成されてなるものである。

【 0 0 0 8 】

かかる構成は、特に、請求項 1 記載の発明に係るインテリジェント中継機器における不正アクセス回避方法を実行するに適したもので、例えば、いわゆるマイクロコンピュータ、又は、それと同等の機能を有する回路とソフトウェアによって実現し得るものである。

【 0 0 0 9 】

【発明の実施の形態】

以下、本発明の実施の形態について、図 1 乃至図 4 を参照しつつ説明する。

なお、以下に説明する部材、配置等は本発明を限定するものではなく、本発明の趣旨の範囲内で種々改変することができるものである。

最初に、本発明の実施の形態におけるインテリジェント中継機器を用いて構成された LAN システムについて、図 1 を参照しつつ説明する。

この LAN システムにおいて、インテリジェント中継機器 1 には、複数の端末としてのいわゆるパーソナルコンピュータ 2 が接続される一方、LAN 基幹線 3 が接続されている。この LAN 基幹線 3 には、少なくとも管理用コンピュータ 4 が接続されるが、さらに、他のネットワーク 5 が接続されてもよい。そして、管理用コンピュータ 4 は、LAN 基幹線 3 に直接接続される形態の他、他のネットワーク 5 を介して接続される形態であってもよい。

なお、管理用コンピュータ 4 は、サーバを兼ねるものであってもよく、また、サーバは管理用コンピュータ 4 とは、別個に設けるようにしてもよい。

また、インテリジェント中継機器 1 は、OS I 参照モデルにおけるネットワーク層を含めてこれより上位の層、換言すれば、TCP / IP (Transmission Control Protocol / Internet Protocol) におけるインターネット層より上位の層におけるパケット処理に対応できるよう構成されてなるものであるとする。

【 0 0 1 0 】

図 2 には、このインテリジェント中継機器 1 の構成例が示されており、以下、

同図を参照しつつ、その構成等について説明する。

このインテリジェント中継機器 1 は、中央制御部 6 と、LAN 基幹線インターフェイス部（図 2 においては「B-I/F」と表記）7 と、ポートインターフェイス部（図 2 においては「P-I/F」と表記）8 と、記憶部 9 とを有し、これらが共通内部バス 10 を介して相互に接続されたものとなっているもので、中央制御部 6 によって後述するような不正アクセス回避処理がなされることを除けば、従来装置と基本的に変わるところはないものである。

かかる構成において、中央制御部 6 は、このインテリジェント中継機器 1 全体の動作制御を行うもので、特に、本発明の実施の形態においては、後述する不正アクセス回避処理が実行されるようになっている。

LAN 基幹線インターフェイス部 7 は、LAN 基幹線 3 と、このインテリジェント中継機器 1 とのいわゆるインターフェイスを図るものであり、また、ポートインターフェイス部 8 は、端末としてのパーソナルコンピュータ 2 とこのインテリジェント中継機器 1 とのいわゆるインターフェイスを図るものである。

記憶部 9 は、中央制御部 6 によって実行される各種のプログラムが記憶されると共に、LAN 基幹線インターフェイス部 7 やポートインターフェイス部 8 を介して取り込まれたデータや、また、これらを介して外部へ送出されるデータなどが記憶されるものとなっている。この記憶部 9 は、電源が断とされても記憶内容が消去されない領域と、電源の断によって記憶内容が消去される領域とを有してなるものとなっており、データなどの用途等に応じて、それぞれの領域に選択的に記憶されるようになっている。なお、このような記憶部 9 は、公知・周知の記憶素子などによって実現され得るもので、その詳細な説明は省略するが、例えば、いわゆる ROM や RAM などの半導体メモリの他、ハードディスク等を用いて構成するのが好適である。

【 0 0 1 1 】

なお、本発明の実施の形態における記憶部 9 には、TCP/IP プロトコルが、電源が断とされても記憶内容が消去されない領域に記憶されており、中央制御部 6 によって必要に応じて実行されるものとなっている。なお、TCP/IP プロトコルには、種々あるが、後述するような不正アクセス回避処理の実行に適す

るものであれば特定のものに限定される必要はなく、より具体的には、ユーザ識別子とパスワードによるいわゆる認証処理が行われるものであることが必要である。

また、この記憶部 9 には、このインテリジェント中継機器 1 に予め付与された IP アドレス、TCP/IP プロトコルに基づく外部の機器からのアクセスに対する認証に必要なユーザ識別子 (ID) とパスワードが、電源が断とされても記憶内容が消去されない領域に予め記憶されている。

【 0 0 1 2 】

次に、中央制御部 6 によって実行される不正アクセス回避処理の第 1 の例について図 3 を参照しつつ説明する。

まず、前提として、この不正アクセス回避処理は、中央制御部 6 において実行されるメインルーチン処理の中で、一つのサブルーチン処理として実行されるようになっているものである。

中央制御部 6 による処理が開始されると、最初に、インテリジェント中継機器 1 へ対して外部からアクセスが生じたか否かが判定され (図 3 のステップ S 1 0 0 参照)、外部からのアクセス発生と判定されると (YES の場合)、次のステップ S 1 0 2 の処理へ進むこととなる。一方、ステップ S 1 0 0 において、外部からのアクセスが無いと判定された場合 (NO の場合) には、一旦、このサブルーチン処理を終了し、図示されないメインルーチン処理へ戻り、メインルーチン処理の所定の処理を経た後、再び、このサブルーチン処理が開始されることとなる。

【 0 0 1 3 】

そして、ステップ S 1 0 2 においては、この外部からのインテリジェント中継機器 1 へ対するアクセスが初回であるか否かが判定され、初回であると判定された場合 (YES の場合) には、次述するステップ S 1 1 0 の処理へ進む一方、初回ではないと判定された場合 (NO の場合) には、後述するステップ S 1 0 4 の処理へ進むこととなる。

ステップ S 1 1 0 においては、外部からインテリジェント中継機器 1 へアクセスを行った外部機器 (例えば、管理用コンピュータ 4) へ対してユーザ識別子 (

I D) とパスワードが要求され、それらの入力受付が行われることとなる。

次いで、入力されたユーザ識別子とパスワードに対する認証処理が行われることとなる（図 3 のステップ S 1 1 2 参照）。

【 0 0 1 4 】

ここで、先のステップ S 1 1 0 及びステップ S 1 1 2 の処理は、公知・周知の T C P / I P プロトコルの実行処理によってなされるものである。すなわち、本発明の実施の形態におけるインテリジェント中継機器 1 は、先にその構成の説明において述べたように、T C P / I P プロトコルが搭載されたものを前提としており、特に、ユーザ識別子とパスワードによる認証処理が行われるものが好適である。このような T C P / I P プロトコルとしては、例えば、TELNET を挙げることができる。なお、このプロトコルの詳細な処理手順についてのここでの説明は省略することとする。

そして、認証処理（図 3 のステップ S 1 1 2 参照）の終了後は、認証が成立したか否かが判定されることとなる（図 3 のステップ S 1 1 4 参照）。ここで、認証の成立とは、ユーザ識別子及びパスワードが記憶部 9 に予め設定されているものと一致し、アクセスを行った外部機器へ対して認証が与えられる場合を言い、認証不成立とは、ユーザ識別子及びパスワードが記憶部 9 に予め設定されているものと一致せず、認証が与えられない場合を言う。

【 0 0 1 5 】

ステップ S 1 1 4 において、認証成立せず、すなわち、認証不成立と判定された場合（N O の場合）には、外部機器に対する応答不可とされて（図 3 のステップ S 1 2 2 参照）、一連のサブルーチン処理を終了し、一旦、メインルーチン処理へ戻ることとなる。そして、メインルーチン処理においては、搭載されている T C P / I P プロトコルに応じて、応答不可に対応する処理がなされることとなる。

一方、ステップ S 1 1 4 において、認証成立と判定された場合（Y E S の場合）には、外部機器からのアクセスに対する応答可とされて（図 3 のステップ S 1 1 6 参照）、次いで、今回の処理が外部機器からの初回のアクセスに対応するものであるか否かが判定されることとなる（図 3 のステップ S 1 1 8 参照）。そし

て、外部機器のアクセスが初回であると判定された場合（YESの場合）には、次述するステップS 1 2 0の処理へ進む一方、外部機器のアクセスが初回ではないと判定された場合（NOの場合）には、既に、次述するステップS 1 2 0の処理が行われており、再度の処理の必要がないため、一連のサブルーチン処理が終了されることとなり、メインルーチン処理へ戻ることとなる。

ステップS 1 2 0の処理においては、外部機器から送信されたパケットに含まれる送信元（外部機器）のIPアドレス（以後「送信元IPアドレス」と言う）が抽出され、記憶部9の所定の領域に記憶されることとなる（図3のステップS 1 1 8参照）。なお、この場合、送信元IPアドレスの記憶領域は、電源が断たされても記憶内容が消去されない領域が好適である。

このステップS 1 2 0の処理が終了した後は、この一連のサブルーチン処理が終了されることとなり、メインルーチン処理へ戻ることとなる。そして、メインルーチン処理においては、搭載されているTCP/IPプロトコルに応じて、応答可に対応する処理がなされることとなる。

【0016】

また、先のステップS 1 0 2において、初回のアクセスではないと判定されてステップS 1 0 4へ進んだ場合には、アクセスを行ってきた外部機器（例えば、管理用コンピュータ4）の送信元IPアドレスが、既に記憶部9に記憶されている送信元IPアドレスと一致するか否かが判定されることとなる。なお、外部機器の送信元IPアドレスは、当該外部機器からインテリジェント中継機器1へ送信されたパケット内に公知・周知の形式で含まれているものを抽出することで認識可能なものである。

そして、このステップS 1 0 4において、送信元IPアドレスが一致すると判定された場合（YESの場合）には、アクセスの有った外部機器に対して応答可とされて、先のステップS 1 1 0の処理へ進むこととなる（図3のステップS 1 0 6参照）。一方、ステップS 1 0 4において、送信元IPアドレスが一致しないと判定された場合（NOの場合）には、外部機器に対する応答不可とされて、一連のサブルーチン処理を終了し、メインルーチン処理へ戻ることとなる（図3のステップS 1 0 8参照）。なお、メインルーチン処理においては、搭載されて

いるTCP/IPプロトコルに応じて、応答不可に対応する処理がなされることとなる。

【0017】

次に、中央制御部6によって実行される不正アクセス回避処理の第2の例について図4を参照しつつ説明する。なお、図3に示された処理と同一の内容の処理については、同一の符号を付してその詳細な説明を省略し、以下、異なる点を中心に説明することとする。

まず、この第2の例における不正アクセス回避処理の内容を概括的に述べれば、先の図3に示された第1の例における不正アクセス回避処理を基本として、アクセスを認める外部機器の送信元IPアドレスに有効期間を設ける一方、送信元IPアドレスが一致しない場合には、不正アクセスIPリストへ記憶すると共に、管理装置へ通知するようにしたものである。

以下、図4を参照しつつ、具体的に説明する。この図4に示されたサブルーチン処理において、図3に示されたサブルーチン処理と異なるのは、ステップS106、S109a、S109bが設けられた点にあり、他の処理内容は図3に示されたサブルーチン処理におけるものと同一であるので、以下、これらの異なる各々のステップの処理内容について説明することとする。

【0018】

まず、ステップS104において、アクセスを行ってきた外部機器（例えば、管理用コンピュータ4）の送信元IPアドレスが、既に記憶部9に記憶されている送信元IPアドレスと一致すると判定された場合（YESの場合）、この送信元IPアドレスが有効期限内のものか否かが判定されることとなる（図4のステップS105参照）。すなわち、このインテリジェント中継機器1に対するアクセスを許容する外部機器の送信元IPアドレスは、既に述べたように記憶部9の所定の領域に予め記憶されるが、その最初の記憶の際に有効期間を定め、ステップS105においては、その有効期限内であるか否かが判定されるようになっている。なお、有効期間を判定するためには、送信元IPアドレスの記憶の時点からの時間の経過を認識する必要があるが、これは、公知・周知のソフトウェア処理によるいわゆるカレンダー機能、または、時計機能が中央制御部6において実

行されるようにすることで実現可能なものである。

そして、ステップ S 1 0 5 において、有効期限内であると判定された場合（YES の場合）には、アクセスの有った外部機器に対して応答可とされて、ステップ S 1 1 0 の処理へ進むこととなる（図 4 のステップ S 1 0 6 参照）。

【 0 0 1 9 】

一方、ステップ S 0 4 において、送信元 IP アドレスが一致しないと判定されたか又は、ステップ S 1 0 5 において、有効期限内ではない、すなわち、換言すれば、有効期限切れであると判定されたか、いずれかの場合には、外部機器に対する応答不可とされて（図 4 のステップ S 1 0 8 参照）、次いで、不正アクセス IP リストへ、ステップ S 1 0 4 の判定において一致しないとされた外部機器の送信元 IP アドレスが登録されることとなる（図 4 のステップ S 1 0 9 a 参照）。すなわち、このインテリジェント中継機器 1 へ外部からのアクセスがあり、そのアクセスしてきた外部機器の送信元 IP アドレスが、ステップ S 1 0 4 の判定において不一致とされた場合に、当該不一致とされた送信元 IP アドレスを登録しておくための不正アクセス IP リストが記憶部 9 の所定の領域に設けられており、そこへ逐次記憶されるようになっている。

次いで、この不一致とされた送信元 IP アドレスを、管理用コンピュータ 4 へ知らしめるべく、この送信元 IP アドレスが所定の packets として、LAN 基幹線インターフェイス部 7 を介して管理用コンピュータ 4 へ送信されることとなる（図 4 のステップ S 1 0 9 b 参照）。そして、このステップ 1 0 9 b の処理後は、メインルーチン処理へ戻り、搭載されている TCP / IP プロトコルに応じて、応答不可に対応する処理がなされることとなる。

【 0 0 2 0 】

なお、上述の第 2 の例においては、不一致とされた送信元 IP アドレスの記憶（図 4 のステップ S 1 0 9 a 参照）と、その送信元 IP アドレスの管理用コンピュータ 4 への通知（図 4 のステップ S 1 0 9 b 参照）とを行うようにしたが、いずれか一方を行うようにしてもよい。

また、上述した第 1 及び第 2 のいずれの例においても、インテリジェント中継機器 1 に記憶されるアクセス可能な外部機器の送信元 IP アドレスは、一つであ

ることを前提として説明をしたが、一つに限定される必要はなく、複数設定されても勿論よいものである。

【0021】

また、インテリジェント中継機器1が、TCP/IPネットワークにおけるネットワーク管理プロトコルであるSNMP(Simple Network Management Protocol)に対応できるよう構成されたものである場合、すなわち、インテリジェント中継機器1にSNMPエージェントが搭載される一方、例えば、管理用コンピュータ4にSNMPマネージャが搭載されると共に、他のコンピュータにも、SNMPマネージャが搭載される場合などにおいては、インテリジェント中継機器1からイベント通知(Trap)を送信する際の送信先として、特定のコンピュータに限定したい場合、例えば、管理用コンピュータ4のみをTrapの送信先としたい場合、その送信元IPアドレスをインテリジェント中継機器1に管理装置情報として記憶しておくことで、管理用コンピュータ4のみにTrapが送信されるようにして、情報の不用意な拡散を防止することができるものとなる。

さらに、例えば、先の図3及び図4におけるステップS110、S112の認証処理を、暗号化してよりセキュリティの向上を図ってもよい。

【0022】

なお、上述の構成例においては、中央制御部6によって実行されるインテリジェント中継機器用不正アクセス回避プログラムは、プログラムの記録媒体としての記憶部9の一部を構成する不揮発性の半導体メモリに記憶されており、この半導体メモリから中央制御部6に読み込まれて実行されることを前提として説明をしたが、記録媒体としては、半導体メモリに限定される必要がないことは勿論である。

すなわち、記録媒体としては、この他、フレキシブルディスクやCD-ROM、また、DVD、PD等の光学記録媒体、MD等の光磁気記録媒体、磁気記録媒体等を用いても良いものである。なお、記録媒体によっては、その記録媒体専用のデータの読み出し、書き込みを行う装置が必要となり、それらを含めて記憶部9を構成しても良いことは勿論である。

【0023】

【発明の効果】

以上、述べたように、本発明によれば、管理用コンピュータの送信元IPアドレスを、既存のTCP/IPプロトコルの実行処理において受信されたパケットから抽出して記憶し、以後、その送信元IPアドレス以外のIPアドレスを有する外部の機器との通信を禁止するようにしたので、従来のTCP/IPプロトコルの認証処理と相俟って、従来に比してよりセキュリティの向上を図ることができ、信頼性の高いシステムを提供することができるという効果を奏するものである。

また、送信元IPアドレスが一致した後にTCP/IPプロトコルによる認証処理を行えばよいので、種々のTCP/IPプロトコルを搭載するものにあっては、いずれか一つのプロトコルによって認証処理が実行されるようにしておくことで十分なセキュリティが保持でき、個々のプロトコルの認証処理を省略することができ、ソフトウェアの負担を軽減することができるという効果を奏するものである。

さらに、ブロードキャストによるアクセスに対する応答も制限することができるので、被管理機器、すなわち、管理用コンピュータによる管理の対象とされたインテリジェント中継機器の存在を、外部からの侵入者にとって識別困難なものにすることができ、従来に比してよりセキュリティの向上が図られることとなる。

また、従来、プロトコル毎に用意していたユーザ識別子やパスワードを一本化することができ、ソフトウェアの簡素化を図ることができるという効果を奏するものである。

【図面の簡単な説明】

【図 1】

本発明の実施の形態におけるLANシステムの構成例を示す構成図である。

【図 2】

図 1 に示されたLANシステムに用いられるインテリジェント中継機器の構成例を示す構成図である。

【図 3】

図 2 に示されたインテリジェント中継機器によって実行される不正アクセス回

避処理の第 1 の例における処理手順を示すサブルーチンフローチャートである。

【図 4】

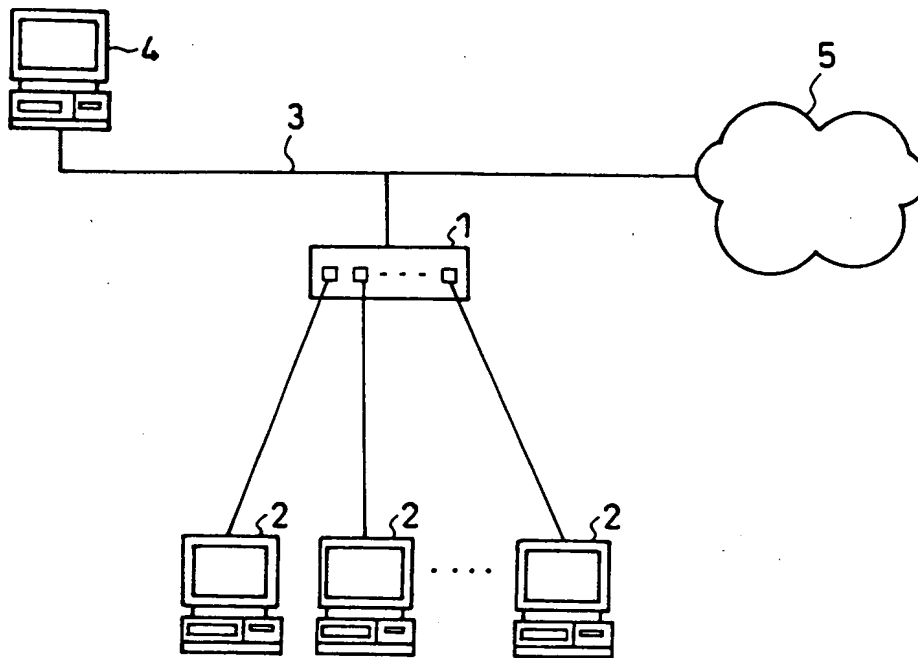
図 2 に示されたインテリジェント中継機器によって実行される不正アクセス回避処理の第 2 の例における処理手順を示すサブルーチンフローチャートである。

【符号の説明】

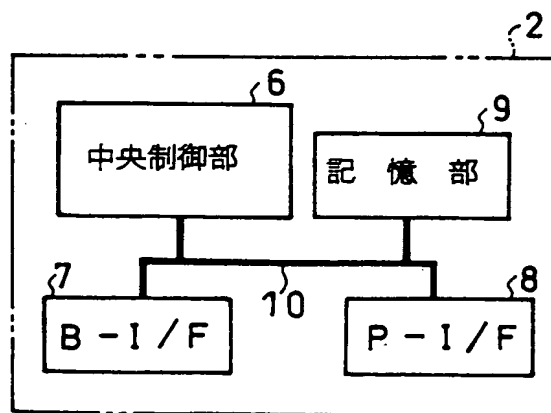
- 1 … インテリジェント中継機器
- 3 … LAN 基幹線
- 4 … 管理用コンピュータ
- 6 … 中央制御部
- 5 … 他のネットワーク
- 7 … LAN 基幹線インターフェイス部
- 8 … ポートインターフェイス部
- 9 … 記憶部

【書類名】 図面

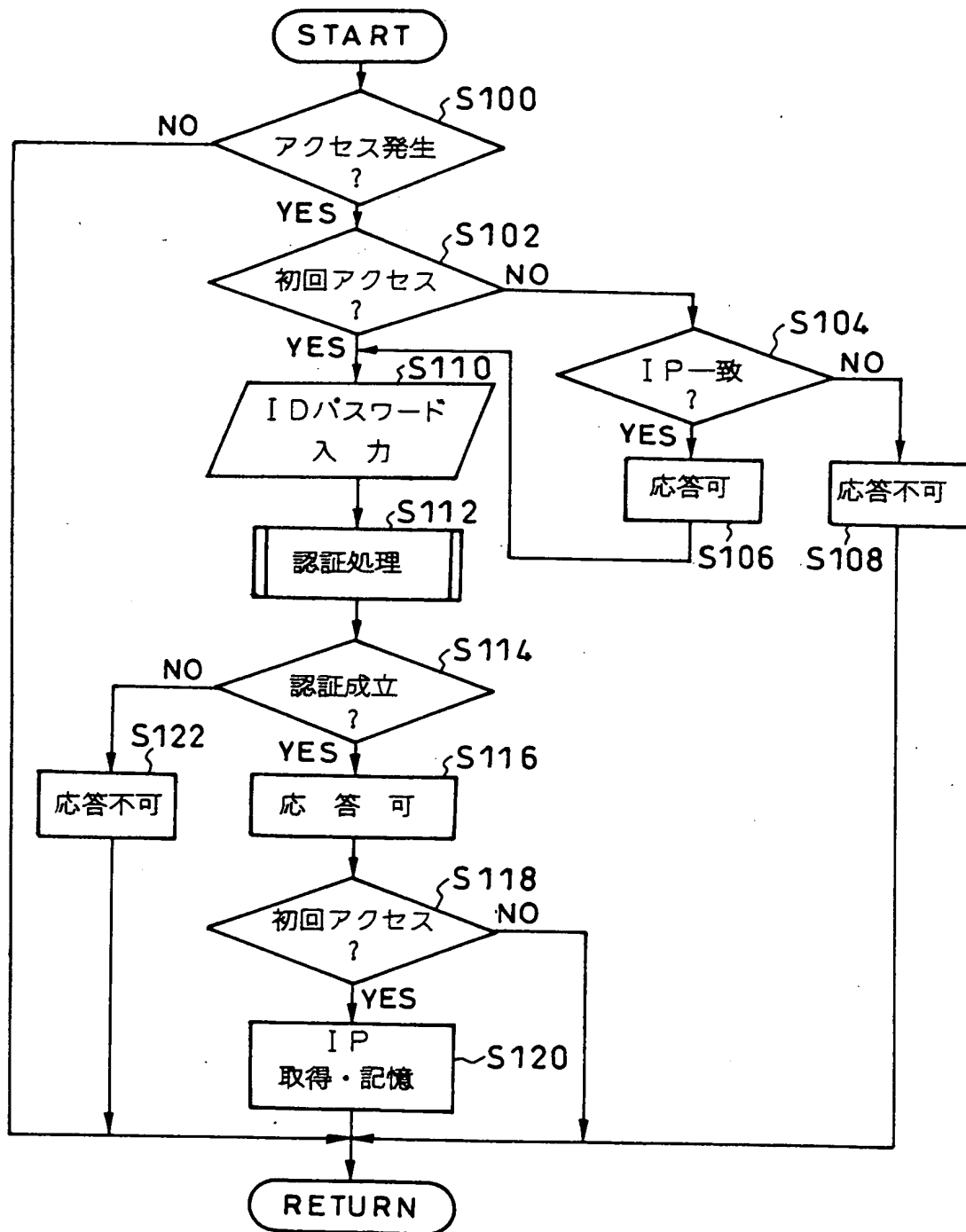
【図 1】



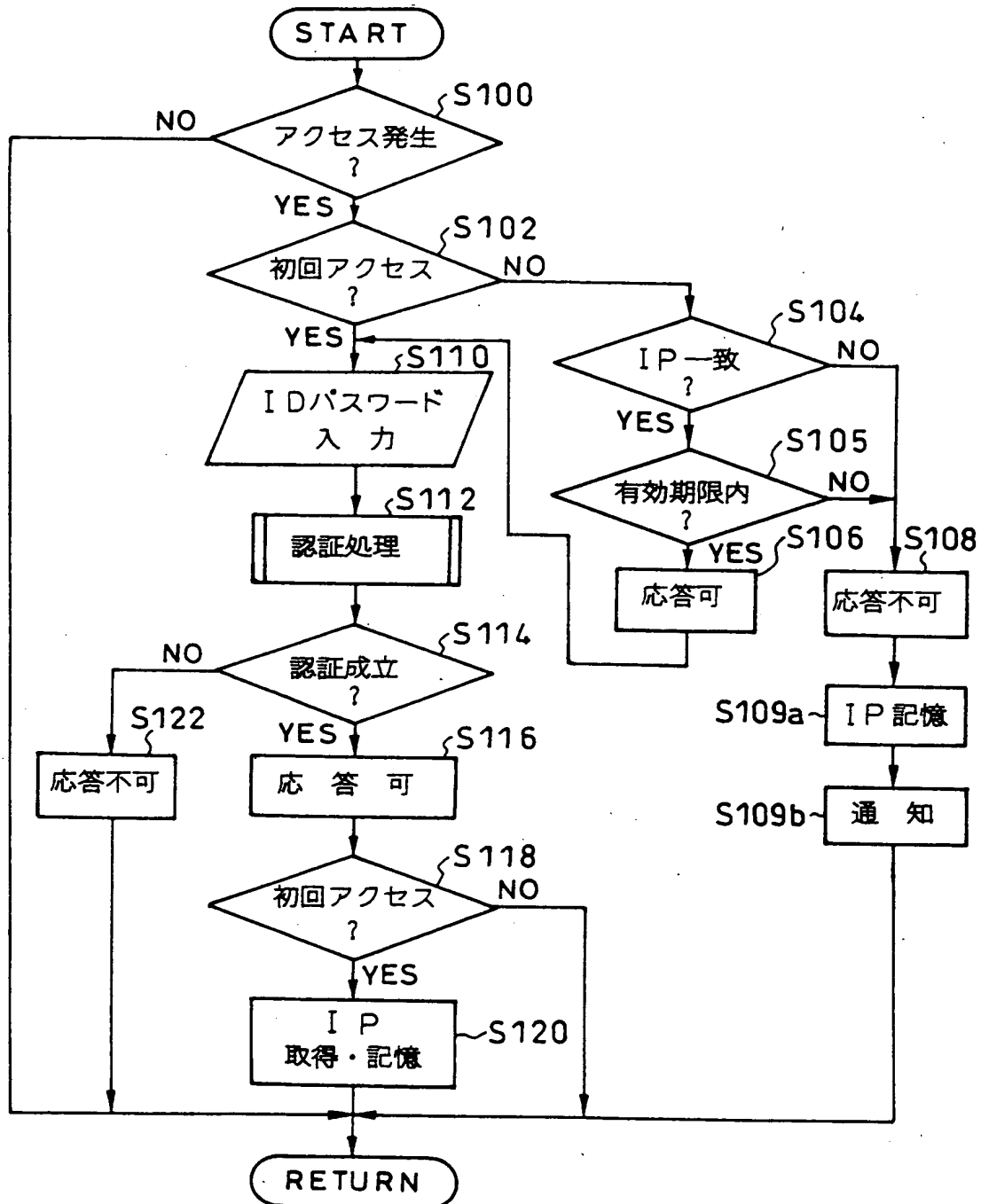
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 既存のソフトウェアに新たな機能を若干付加するだけで、セキュリティ機能の強化、信頼性の向上を図る。

【解決手段】 インテリジェント中継機器に対して外部の機器から最初にアクセスがあり、その外部の機器がインテリジェント中継機器におけるTCP/IPプロトコルに基づく認証処理によって認証を得た場合、インテリジェント中継機器は、その外部の機器の送信元IPアドレスを記憶し（ステップS114, S116, S118, S120）、以後、外部からアクセスが生じた場合、その送信元IPアドレスが、先に記憶された送信元IPアドレスと一致した場合にのみ、そのアクセスに対する応答を可能として（ステップS104, S106）、セキュリティの向上が図られている。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [396008347]

1. 変更年月日 2000年10月24日

[変更理由] 住所変更

住 所 東京都品川区西五反田7-22-17 TOCビル

氏 名 アライドテレシス株式会社